Remarks

Reconsideration of the above-captioned application is respectfully requested. Claims 1-7, 11, and 13 have been rejected under 35 U.S.C. §102 as being anticipated by Zhang, and the remaining claims have been rejected under 35 U.S.C. §103 as being obvious over Zhang. Claim 4 essentially has been rewritten in independent form, and Claims 1-3 cancelled, so that Claims 4-17 remain pending.

In the previous rejection, Enichen, now disqualified as prior art, was combined with Zhang in the obviousness rejections. Since Applicant removed Enichen as prior art the examiner simply alleges that the now-missing pieces from Zhang are obvious, without any evidence of record to support this contention. Absent evidence to support a finding of fact, the rejection is reversible error.

Furthermore, the rejection reflects an erroneous factual reading of Zhang, as consultation with the present inventor, a well-regarded leader in the field of cryptography, indicates. Specifically, Zhang seeks to solve the so-called "code book" attack, in which even if the key or cipher is unknown, if the same words always produce the same ciphertext a frequency analysis can be performed to deduce what the words mean. This attack is defeated by Zhang's cipher block chaining, in which a word's scrambled version is always different because it depends on what preceded it in the message. Zhang, because it uses a pseudo one-time pad, further embellishes the code book attack solution by performing forward and backward chaining, so that even the first part of the message cannot be defeated by the code book attack. Importantly, the relied-upon portion of Zhang does one thing - chaining, using cipher chaining instead of plan text chaining - and not two things, namely, both chaining and, separate from the chaining process, running rounds of a cipher.

In contrast, the present claims in various ways not only require both chaining and running rounds of a cipher, they recite alternating the running of the rounds of the cipher with running the chaining mode, something never before done or suggested to the best of Applicant's knowledge and certainly not suggested in the references of record. For instance, Claim 13 requires scrambling a block using one and only one round of a cipher, ***then*** chaining the block to another block to render a chained block, ***then*** scrambling the chained block using one and only round of the cipher, something that the relied-upon section of Zhang does not do. Instead, the relied-upon section of Zhang performs all of the chaining without scrambling between chainings. The fact that Zhang uses cipher chaining and not plain text chaining should not confuse the reader that Zhang scrambles within rounds of chainings, when in fact it does not do so. Indeed, the fact that Zhang uses cipher chaining and not plain text chaining as required by, e.g., Claim 1, is another difference not touched on in the rejection and further militates toward patentability.

With the above analysis in mind, the factual errors underpinning the allegations regarding Zhang render the rejections reversible on appeal. It is respectfully asserted that the claims as they stand are allowable.

For the record, Applicant does not acquiesce in the comments about the specification.

The Examiner is cordially invited to telephone the undersigned at (619) 338-8075 for any reason which would advance the instant application to allowance.